

HIPAA Business Associate Agreement (BAA)

BAA in which the County is the Business Associate of the Department of Alcohol and Drug Programs

Preamble

This addendum is intended to meet ADP's responsibility as a covered entity to obtain the satisfactory assurances required by 45 CFR 164.502(e), to the extent that County is a business associate of ADP. This addendum is not intended to duplicate or expand County's existing obligations as a covered entity to any extent not required by law.

ADP and County shall cooperate to assure mutual agreement as to those transactions between them to which this Addendum applies, i.e., to identify those situations in which County is or is not ADP's business associate. For example, County and ADP have agreed in concept that County is not regarded as ADP's business associate with regard to PHI created in County's own alcohol and other drug abuse programs, because that PHI and the various transactions related to it are already covered by County's obligations as a covered entity. That is, this Addendum is not intended to duplicate or expand County's HIPAA obligations with regard to situations, PHI or persons where County already has HIPAA obligations by virtue of being a health care provider.

This Addendum is also intended to meet the requirements of 42 CFR 2.53, to allow County to act on ADP's behalf in handling PHI pursuant to ADP's authority and obligation to perform audit and evaluation activities. As with County's HIPAA obligations, this Addendum is not intended to expand or duplicate County's existing obligations arising under 42 CFR Part 2 to any extent not required by law.

In the event of any conflict between the obligations arising under this Addendum pursuant to HIPAA and those arising under 42 CFR Part 2, the provision which is more protective of a patient's confidentiality or other rights will prevail. ADP and County will cooperate to determine the controlling provisions as the need arises.

County and ADP agree to continue negotiations to simplify and clarify this Addendum, to the end that all PHI moving between them will be adequately safeguarded and maintained as confidential, as required by law, while minimizing the duplication of obligations and unnecessary expansion of obligations of either County or ADP.

1. Recitals

A. COVERED ENTITY

A covered entity means a health plan, a health care clearinghouse, or a health care provider that conducts any standard electronic transaction. The standard electronic transactions are those provided in the Transactions and Code Sets Rule.

B. BUSINESS ASSOCIATE

A Business Associate (BA) means a person or organization, other than a member of the covered entity's workforce, which performs or assists in the performance of:

A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing, or any other function or activity regulated by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, or legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.

BA's perform these functions on **behalf** of covered entities or to an Organized Health Care Arrangement. A covered entity can be a BA of another covered entity.

- C. This Contract (Agreement) has been determined to constitute a BA relationship under the HIPAA and its implementing privacy and security regulations at 45 CFR Parts 160 and 164 (HIPAA Regulations).
- D. The California Department of Alcohol and Drug Programs (ADP) wishes to disclose to the BA certain information pursuant to the terms of this Agreement, some of which may constitute Protected Health Information (PHI).
- E. PHI means any information, whether oral or recorded in any form or medium that relates to the past, present, or future physical or mental condition of an individual, the provision of health and dental care to an individual, or the past, present, or future payment for the provision of health and dental care to an individual; and that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. PHI shall have the meaning given to such term under HIPAA and HIPAA Regulations, as the same may be amended from time to time.
- F. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI, or confidential data that is essential to the ongoing operation of the BA's organization and intended for internal use; or interference with system operations in an information system.
- G. As set forth in this Agreement, Contractor, here and after, is the BA of ADP that provides services, arranges, performs or assists in the performance of functions or activities on behalf of ADP and creates, receives, maintains, transmits, uses or discloses PHI.
- H. ADP and BA desire to protect the privacy and provide for the security of PHI created, received, maintained, transmitted, used or disclosed pursuant to this Agreement, in compliance with HIPAA and HIPAA Regulations and other applicable laws, including 42 CFR Part 2.
- I. The purpose of the Addendum is to satisfy certain standards and requirements of HIPAA the HIPAA Regulations.
- J. The terms used in this Addendum, but not otherwise defined, shall have the same meanings as those terms in the HIPAA Regulations.

In exchanging information pursuant to this Agreement, the parties agree as follows:

2. Permitted Uses and Disclosures of PHI by Business Associate

- A. Permitted Uses and Disclosures. Except as otherwise indicated in this Addendum, BA may use or disclose PHI only to perform functions, activities or services specified in this Agreement, for, or on behalf of ADP, or as required by law.
- B. Specific Use and Disclosure Provisions. Except as otherwise indicated in this Addendum, BA may:
 - 1) Use and disclose for management and administration. Use and disclose PHI for the proper management and administration of the BA or to carry out the legal responsibilities of the BA, provided that disclosures are required by law, or the BA obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and will be used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the BA of any instances of which it is aware that the confidentiality of the information has been breached.

3. Responsibilities of Business Associate

Business Associate agrees:

- A. Nondisclosure. Not to use or disclose PHI other than as permitted or required by this Agreement or as required by law. ADP advises BA that 42 CFR Part 2 generally prohibits any re-disclosure without either the written consent of the person to whom the information pertains or a court order that complies with 42 CFR Part 2, Subpart E.
- B. Safeguards. To implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI, including electronic PHI, that it creates, receives, maintains, uses or transmits on behalf of ADP; and to prevent use or disclosure of PHI other than as provided for by this Agreement. BA shall develop and maintain a written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the BA's operations and the nature and scope of its activities, and which incorporates the requirements of Section C, Security, below. BA will provide ADP with its current and updated policies.
- C. Security. To take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI, and provide data security procedures for the use of ADP at the end of the contract period. These steps shall include, at a minimum:
 - 1) Complying with all of the data system security precautions listed in this Agreement or in an Exhibit attached to this Agreement;
 - 2) Achieving and maintaining compliance with the HIPAA Security Rule 45 CFR Parts 160 and 164, as necessary in conducting operations on behalf of ADP under this Agreement;

3) Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III-Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies; and

4) Complying with the safeguard provisions in the ADP's Information Security Policy, embodied in Health Administrative Manual, Sections 6-1000 et seq. and in the Security and Risk Management Policy in the Information Technology Section of the State Administrative Manual, Sections 4840 et seq., in so far as the security standards in these manuals apply to BA's operations. In case of a conflict between any of the security standards contained in any of these four enumerated sources of security standards, the most stringent shall apply. The most stringent means that safeguard which provides the highest level of protection to PHI from unauthorized disclosure. Further, BA must comply with changes to these standards that occur after the effective date of this Agreement.

Business Associate shall designate a Security Officer to oversee its data security program who shall be responsible for carrying out the requirements of this section and for communicating on security matters with ADP.

- D. Mitigation of Harmful Effects. To mitigate, to the extent practicable, any harmful effect that is known to BA of a use or disclosure of PHI by BA or its subcontractors in violation of the requirements of this Addendum.
- E. Business Associate's Agents. To ensure that any agents, including subcontractors, to whom BA provides PHI received from or created or received by BA on behalf of ADP, agree to the same restrictions and conditions that apply to BA with respect to such PHI, including implementation of reasonable and appropriate administrative, physical, and technical safeguards to protect such PHI; and to incorporate, when applicable, the relevant provisions of this Addendum into each subcontract or subaward to such agents or subcontractors.
- F. Availability of Information to ADP and Individuals. To provide access as ADP may require, and in the time and manner designated by ADP (upon reasonable notice and during BA's normal business hours) to PHI in a Designated Record Set, to ADP (or, as directed by ADP), to an individual, in accordance with 45 CFR Section 164.524. Designated Record Set means the group of records maintained for ADP that includes medical, dental and billing records about individuals; enrollment, payment, claims adjudication, and case or medical management systems maintained for ADP health plans; or those records used to make decisions about individuals on behalf of ADP. Business Associate shall use the forms and processes developed by ADP for this purpose and shall respond to requests for access to records transmitted by ADP within fifteen (15) calendar days of receipt of the request by producing the records or verifying that there are none.
- G. Amendment of PHI. To make any amendment(s) to PHI that ADP directs or agrees to pursuant to 45 CFR Section 164.526, in the time and manner designated by ADP.
- H. Internal Practices. To make BA's internal practices, books and records relating to the use and disclosure of PHI received from ADP, or created or received by BA on behalf of ADP, available to ADP or to the Secretary of the U.S. Department of Health and Human Services in a time and manner designated by ADP or by the Secretary, for purposes of determining ADP's compliance with the HIPAA Regulations.

- I. Documentation of Disclosures. To document and make available to ADP or (at the direction of ADP) to an individual such disclosures of PHI, and information related to such disclosures, necessary to respond to a proper request by the subject individual for an accounting of disclosures of PHI, in accordance with 45 CFR 164.528.
- J. Notification of Breach. During the term of this Agreement:
- 1) Discovery of Breach. To notify ADP **immediately by telephone call plus e-mail or fax** upon the discovery of breach of security or privacy of PHI in electronic or paper form if the PHI was, or is reasonably believed to have been, acquired by an unauthorized person; or **within 24 hours by e-mail or fax** of any suspected security incident, intrusion or unauthorized use or disclosure of PHI in violation of this Agreement and this Addendum, or potential loss of confidential data affecting this Agreement. Notification shall be provided to the ADP contract manager, the ADP Privacy Officer and the ADP Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves electronic PHI, notification shall be provided by calling the ADP ITSD Help Desk at (916) 327-3010. Business Associate shall take:
 - i. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and,
 - ii. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.
 - 2) Investigation of Breach. To immediately investigate such security incident, breach, or unauthorized use or disclosure of PHI or confidential data. Within 72 hours of the discovery, to notify the ADP contract manager, the ADP Privacy Officer, and the ADP Information Security Officer of:
 - i. What data elements were involved and the extent of the data involved in the breach;
 - ii. A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed PHI or confidential data;
 - iii. A description of where the PHI or confidential data is believed to have been improperly transmitted, sent, or utilized;
 - iv. A description of the probable causes of the improper use or disclosure; and,
 - v. Whether Civil Code Sections 1798.29 or 1798.82 or any other federal or state laws requiring individual notifications of breaches are triggered.
 - 3) Written Report. To provide a written report of the investigation to the ADP contract manager, the ADP Privacy Officer, and the ADP Information Security Officer within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report shall include, but not be limited to, the information specified above, as well as a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure.
 - 4) Notification of Individuals. To notify individuals of the breach or unauthorized use or disclosure when required under state or federal law and to pay any costs of such notifications, as well as any costs associated with the breach. The ADP contract manager, the ADP Privacy Officer, and the ADP Information Security Officer shall approve the time, manner and content of any such notifications.

- 5) ADP Contact Information. To direct communications to the above referenced ADP staff, the Contractor shall initiate contact as indicated herein. Initial contact shall be made to the ADP Privacy Officer, followed by the ADP Manager for the Fiscal Management and Accountability Branch and then the ADP Information Security Officer. To the extent possible, contact should be made to all three individuals. ADP reserves the right to make changes to the contact information below by giving written notice to the Contractor. Said changes shall not require an amendment to this Agreement or Addendum.

ADP Privacy Officer	Daryl Brown, Privacy Officer ADP 1700 K Street, Sacramento, CA 95811 Telephone: (916) 323-1865 E-mail: dbrown@adp.ca.gov
ADP Manager for Fiscal Management and Accountability Branch	Susan King, Manager ADP 1700 K Street, Sacramento, CA 95811 Telephone: (916) 323-6698 E-mail: sking@adp.ca.gov
ADP Information Security Officer	Gary Hummel, Security Officer ADP 1700 K Street, Sacramento, CA 95811 Telephone: (916) 327-6724 E-mail: ghummel@adp.ca.gov

- K. Employee Training and Discipline. To train and use reasonable measures to ensure compliance with the requirements of this Addendum by employees who assist in the performance of functions or activities on behalf of ADP under this Agreement and use or disclose PHI; and discipline such employees who intentionally violate any provisions of this Addendum, including by termination of employment.

- L. **To resist, in judicial proceedings if necessary, any effort to obtain access to the protected information except as expressly provided for in 42 CFR Part 2 and/or other applicable laws.**

4. Obligations of ADP

ADP agrees to:

- A. Notice of Privacy Practices. Provide BA with the Notice of Privacy Practices that ADP produces in accordance with 45 CFR 164.520, as well as any changes to such notice. The most current Notice of Privacy Practices is available at: <http://www.adp.ca.gov/hipaa>.
- B. Permission by Individuals for Use and Disclosure of PHI. Provide the BA with any changes in, or revocation of, permission by an individual to use or disclose PHI, if such changes affect the BA's permitted or required uses and disclosures.
- C. Notification of Restrictions. Notify the BA of any restriction to the use or disclosure of PHI that ADP has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect the BA's use or disclosure of PHI.

- D. Requests Conflicting with HIPAA Rules. Not request the BA to use or disclose PHI in any manner that would not be permissible under the HIPAA Regulations if done by ADP.
- E. Patient identifying information obtained by ADP as an oversight agency and used for audit and evaluation will be maintained in accordance with the security requirements provided in 42 CFR 2.16 and destroyed upon completion of the audit or evaluation. ADP also agrees to comply with the limitations on disclosure and use contained in 42 CFR 2.53(d).

5. Audits, Inspection and Enforcement

From time to time, ADP may inspect the facilities, systems, books and records of BA to monitor compliance with this Agreement and this Addendum. BA shall promptly remedy any violation of any provision of this Addendum and shall certify the same to the ADP Privacy Officer in writing. The fact that ADP inspects, or fails to inspect, or has the right to inspect, BA's facilities, systems and procedures does not relieve BA of its responsibility to comply with this Addendum, nor does ADP's:

- A. Failure to detect, or
- B. Detection, but failure to notify BA or require BA's remediation of any unsatisfactory practices, constitutes acceptance of such practice or a waiver of ADP's enforcement rights under this Agreement and this Addendum.

6. Termination

- A. Termination for Cause. Upon ADP's knowledge of a material breach of this Addendum by BA, ADP shall:
 - 1) Provide an opportunity for BA to cure the breach or end the violation and terminate this Agreement if BA does not cure the breach or end the violation within the time specified by ADP;
 - 2) Immediately terminate this Agreement if BA has breached a material term of this Addendum and cure is not possible; or
 - 3) If neither cure nor termination is feasible, report the violation to the Security of the U.S. Department of Health and Human Services.
- B. Judicial or Administrative Proceedings. BA will notify ADP if it is named as a defendant in a criminal proceeding for a violation of HIPAA. ADP may terminate this Agreement if BA is found guilty of a criminal violation of HIPAA. ADP may terminate this Agreement if a finding or stipulation that the BA has violated any standard or requirement of HIPAA, or other security or privacy laws is made in any administrative or civil proceeding in which the BA is a party or has been joined.
- C. Effect of Termination. Upon termination or expiration of this Agreement for any reason, BA shall return or destroy all PHI received from ADP (or created or received by BA on behalf of ADP) that BA still maintains in any form, and shall retain no copies of such PHI or, if return or destruction is not feasible, shall continue to extend the protections of this Addendum to such information, and shall limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate.

7. Miscellaneous Provisions

- A. Disclaimer. ADP makes no warranty or representation that compliance by BA with this Addendum, HIPAA, or the HIPAA regulations will be adequate or satisfactory for BA's own purposes or that any information in BA's possession or control, or transmitted or received by BA, is or will be security from unauthorized use or disclosure. BA is solely responsible for all decisions made by BA regarding the safeguarding of PHI.
- B. Amendment. The parties acknowledge that federal and state laws relating to electronic data security and privacy are rapidly evolving and that amendment of this Addendum may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HIPAA regulations and other applicable laws relating to the security or privacy of PHI. Upon ADP's request, BA agrees to promptly enter into negotiations with ADP concerning an amendment to this Addendum embodying written assurances consistent with the standards and requirements of HIPAA, the HIPAA regulations or other applicable laws. ADP may terminate this Agreement upon thirty (30) days written notice in the event:
- 1) Business Associate does not promptly enter into negotiations to amend this Addendum when requested by ADP pursuant to this Section; or
 - 2) BA does not enter into an amendment providing assurances regarding the safeguarding of PHI that ADP, in its sole discretion, deems sufficient to satisfy the standards and requirements of HIPAA and the HIPAA Regulations.
- C. Assistance in Litigation or Administrative Proceedings. BA shall make itself and any subcontractors, employees or agents assisting BA in the performance of its obligations under this Agreement, available to ADP at no cost to ADP to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against ADP, its directors, officers or employees based upon claimed violation of HIPAA, the HIPAA regulations or other laws relating to security and privacy, which involves inactions or actions by the BA, except where BA or its subcontractor, employee or agent is a named adverse party.
- D. No Third-Party Beneficiaries. Nothing expressed or implied in the terms and conditions of this Addendum is intended to confer, nor shall anything herein confer, upon any person other than ADP or BA and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.
- E. Interpretation. The terms and conditions in this Addendum shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HIPAA regulations and applicable state laws. The parties agree that any ambiguity in the terms and conditions of this Addendum shall be resolved in favor of a meaning that complies and is consistent with HIPAA and the HIPAA regulations.
- F. Regulatory References. A reference in the terms and conditions of this Addendum to a section in the HIPAA Regulations means the section as in effect or as amended.
- G. Survival. The respective rights and obligations of BA under Section 6.C of this Addendum shall survive the termination or expiration of this Agreement.

- H. No Waiver of Obligations. No change, waiver or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion.